# Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 23:17:56 UTC



## Tool: TONEDEAF 2.0

| | |
|---|---|
| Names | TONEDEAF 2.0 |
| Category | Malware |
| Type | Reconnaissance, Backdoor, Tunneling, Info stealer, Exfiltration |
| Description | (Intezer) At first glance, “Client update.exe” seems like a completely new backdoor malware. However, further examination reveals it’s most likely a highly modified version of the previously seen TONEDEAF backdoor. TONEDEAF is a backdoor that communicates with its Command and Control server via HTTP in order to receive and execute commands. It was mentioned in FireEye’s recent report about an ongoing APT34 operation, as one of the group’s custom tools. We have named the new variant TONEDEAF 2.0.<br><br>TONEDEAF 2.0 is an advanced version of TONEDEAF, serving the same purpose as the original, but with a revamped C2 communication protocol and a substantially modified code base. In contrast to the original TONEDEAF, TONEDEAF 2.0 contains solely arbitrary shell execution capabilities, and doesn’t support any predefined commands. It’s also more stealthy and contains new tricks such as dynamic importing, string decoding, and a victim deception method. |
| Information | <https://intezer.com/blog/apt/new-iranian-campaign-tailored-to-us-companies-uses-updated-toolset/> |

Last change to this tool card: 20 April 2020

Download this tool card in JSON format

### All groups using tool TONEDEAF 2.0

| Changed | Name | Country | Observed |
|---|---|---|---|
| **APT groups** | | | |

| | | | | |
|---|---|---|---|---|
| | OilRig, APT 34, Helix Kitten, Chrysene |  | 2014-Sep 2024 |  |

*1 group listed (1 APT, 0 other, 0 unknown)*

---

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=23cf2c05-faff-48b6-91af-4fc9158edbec